An Application Layer Firewall

Anukriti Raj, Aniruddha Bhattacharjya

Abstract- The project is aimed at developing an APPLICATION LAYER FIREWALL. The firewall is inserted between the premises network and the Internet to establish a controlled link and erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and audit can be imposed. Firewall is being made using JAVA programming language. It will be a total software product that will have an implementation of two proxies for the protocols HTTP and FTP respectively. The project involves building up of a graphical user interface at the front end and source coding of the backend which is done using JAVA language in NetBeans IDE 7.1.2.

Index Terms- HTTP, FTP, Packet, Socket, Port, TCP, OSI-Model, Proxy Server, Swing, Awt,

1. INTRODUCTION

The explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. Protection of data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network based attacks had become a major issue.

Objective of this paper is to study and design an application layer firewall that will implement two proxies HTTP and FTP. The firewall will be able to filter information based on application specific commands and as well as on port number and source and destination IP addresses of the packets. The scope of this Application Layer firewall will be protection of the internal user from the un-trusted outside network. Java is used for the development of this application layer firewall.

1.2. Brief description of firewall

A firewall defines a single chokepoint that keeps the unauthorized users out of the protected network. It protects the system from various kinds of IP spoofing and routing attacks.

A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system. A firewall can also be used for network address translation, which maps local address to Internet addresses, and a network management function that audits or logs Internet usage. Using tunnel mode capability the firewall can be used to implement virtual private networks

1.3. WORKING OF FIREWALL

A firewall acts as a filter that examines the packets that are moving in and out of the network. Any packet that is suspected is always discarded. It is deployed in the gateway or the proxy machines through which the proxy machines through which the Inter-network traffic happens.

Firewalls allows network administrator to offer access to specific types of Inter-network to selected LAN users. This selectivity is a essential part of any information management program, and involves not only protecting private information assets, but also knowing who has access to what.

The project implements the third generation of firewall-Application Layer Firewall based on the protocols HTTP and FTP.

1.4. TYPES OF FIREWALL

❖ There are three common types of Firewalls, namely:

➢ **Packet-filtering routers**

It controls the data that flow to and from the network. In IP networking, the information is sent across the network in the form of pieces of data called packets .Routers are the basic devices that interconnect the IP network. The packet filtering

- ***Anukriti Raj*** *is currently pursuing bachelors degree program in computer science and engineering in ASET, Amity University, Noida, India, PH- . E-mail: anukritiraj.14@gmail.com*
- ***Aniruddha Bhattacharjya*** *is currently working as Assistant Professor Grade II, Department of Computer Science & Engineering, Amity School of Engineering & Technology, Amity University, Noida India, PH-**08130603974**. E-mail: abhattacharjya@amity.edu, abjucse@gmail.com*

routers are programmed according to the security policy. Packet-filtering routers apply a set of rules to each incoming and outgoing IP packet and accordingly it forwards or discards the packet. The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. It is simple, transparent and offers high speed but it lacks authentication. It is difficult to set up packet filtering rules.

- **Application-level gateways**

It is also called PROXY SERVER. It acts as a relay of application-level traffic. It operates at the application layer of the protocol stack. It blocks the packets which do not meet the configured policy of the firewall.
It needs to scrutinize only a few allowable applications. It is implemented through software running on a host or a stand-alone piece of network hardware. In this project an application level gateway is created.
The only disadvantage of application level gateway is additional processing overhead on each connection.

- **Circuit-level gateways**

It operates at the session layer of the OSI model. Two TCP connections are set-up. Circuit level gateways relay TCP segments from one connection to another without examining the contents. The security function consists of determining which connection will be allowed.
It is used in situations where the system administrator trusts the internal user or used for hiding information about protected networks. It is inexpensive. The only drawback of circuit-level gateway is that it does not examine individual packet.

1.5. WHY AN APPLICATION LAYER FIREWALL

One may ask why to use an application layer firewall when there is a disadvantage of slow processing by the application proxies. Well, this firewall will perform filtering based on source IP addresses, destination IP addresses, and source and destination port number.
The inclusion of filtering based on the IP addresses reduce the bottleneck created by slow processing by the application proxies. Thus, the filtering time is reduced to some extent. The application that is configured to be web proxy will allow only http and ftp related traffic.

2. REQUIREMENTS ANALYSIS

2.1. Hardware Requirements

- Pentium Processor
- Colour Monitor
- 64 MB Ram
- 4 GB HDD
- Keyboard
- Internet connection

2.2. Software Requirements

- Java Virtual Machine(JVM)
- Browser
- FTP Server
- FTP Client
- HTTP Server
- HTTP Client
- PROXY SERVER

In the application gateway there has to be proxy protocol. Failure to have proxy may prevent a protocol from being handled correctly by the firewall.
A proxy server for a particular protocol or set of protocols runs dual. The user's client program talks to this proxy server instead of directly to the "real" server on the internet. The proxy server evaluates requests from the client and decides which to pass and to disregard. If the request is approved, the proxy server talks to the real server on behalf of the client (thus the term "proxy"), and proceeds to relay requests from the client to the real server, and to relay the real servers answers back to the client.

3. METHODS AND IMPLEMEMENTATIONS

- The basic idea of this project is that the client sends request to the proxy server. It is a Concurrent Server so multiple requests can be handled simultaneously. It waits for requests and grants connection, if the request is valid. It is implemented using in JAVA language using the concept of thread. Waiting threads remain in the waiting queue and each and every thread is processed by the sever.
- At the proxy server, a rule base manager is acting. Rule Base Manager implies the set of rule implemented by our firewall. The administrator defines these rules. The entire working of this firewall is dependent on the rule base. For this project we are working towards the implementation of two proxies i.e. http and ftp. Hence, rules are defined by the administrator for http and **ftp** protocol only .Also, Rule base manager, manages the tables & files that store the list of blocked websites and IP address.

- The outgoing request sent by the user is checked by the rule base manager at the proxy server. If the request passes all the criterions of the rule base manager, then the request is sent to the server else the request is denied. Corresponding success and error messages are shown to the user by the firewall
- The incoming response from the server is filtered by the rule base and if all the criterions of the rule base are satisfied then access is granted else access to the incoming response is denied. Corresponding success and error messages are shown to the user.

On implementation, this firewall provides effective means to filter the content, blocking IP addresses and blocking certain websites.

.

For the implementation of the above mentioned description JAVA is selected as it is a robust, secure and platform independent language. An application named **FIREWALL VERSION 1.0** is created.

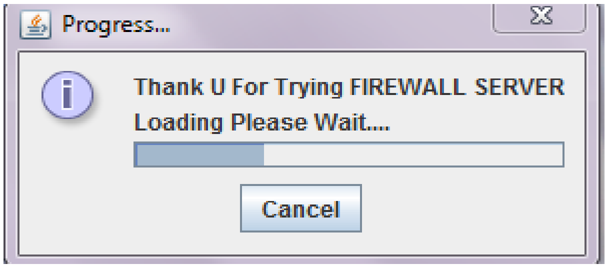
Java provides ***swing*** and ***awt*** package. These packages are used to create a GUI environment for the user. Using swing and awt, different windows are created wherein the administrator enters various information. By Clicking on various tabs of the main menu, different windows appear. On the various opened windows, the user is prompted to enter details like blocked IP address, blocked websites, which ftp server to access, which http server to access, etc. Proper programming is done for storing, updating, deletion and traversing of this information. The administrator can also view the current session and the previous sessions.

The **net** package provides the classes for implementing networking applications. It helps in creation of the server and proxy classes. Using the net package, programming is done for providing access or denial to the requests and responses where the server class refers to the information provided by the administrator and then act accordingly.

4. RESULTS OBTAINED

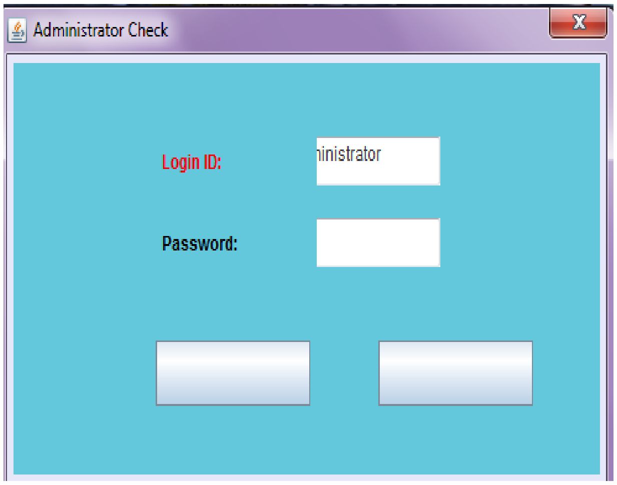
<u>The firewall product so developed will look like the following screenshots:</u>

4.1. This is the first dialog box that appears



Thank U For Trying FIREWALL SERVER
Loading Please Wait....

4.2. This is the second dialog box
Type "administrator" as the user name and "anukriti" password click ok.



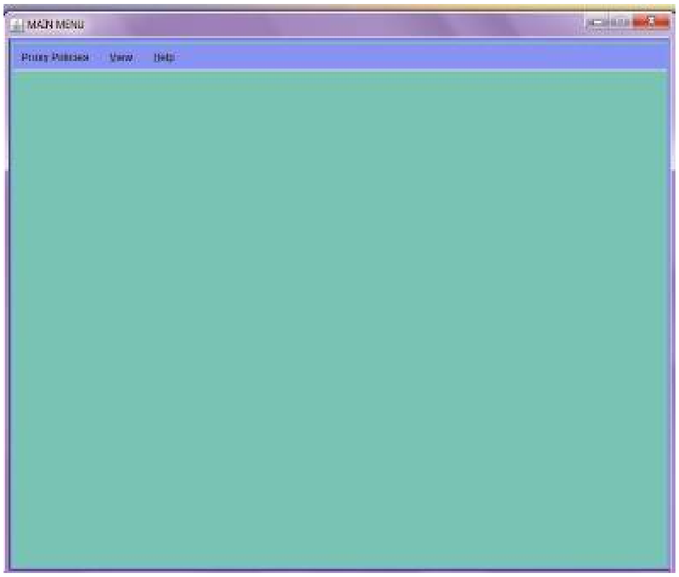
Login ID: ninistrator
Password:

4.3. This is the third dialog box that pops up after log in and it shows the **main menu.**

After successful login the above screen appears.

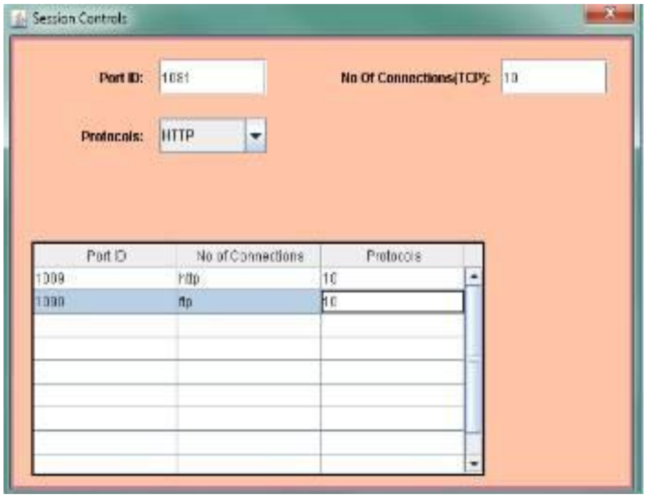
- To start the HTTP proxy server, from Main Menu go to proxy policies-> HTTP policies-> start and view, the session viewer window will appear.
- To start the FTP proxy server, from the Main Menu go to the proxy policies-> FTP policies-> start FTP server. A dialog box asking FTP server name will appear. Enter the FTP server name and click OK, the FTP session viewer window will appear.

- After starting the proxies to view the sessions go to View-> HTTP session Status/FTP session Status. The respective session viewer window will appear.



4.4. It shows the “**session controls**” dialog box where we can mention various details for the rule base of our firewall’s session.

- First go to Proxy policies on the menu bar then click session control.
- For creating sessions enter port ID, no. of connections, and select the protocol.
- Click on add, the respective entry will appear in the table.
- Similarly for removing an entry select that entry from table and click remove.



Port ID: 1081

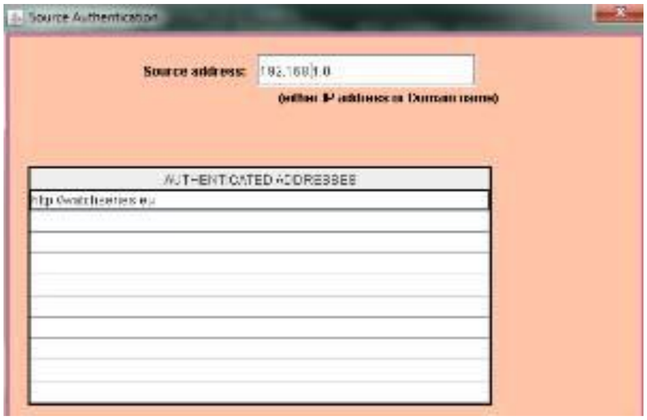
No Of Connections(TCP): 10

Protocols: HTTP

Port ID	No of Connections	Protocols
1009	http	10
1080	ftp	10

4.5. It shows the **source authentication** dialog box.

- First go to Proxy policies on the menu bar then click HTTP policies and click source Authentication,.
- For adding a new source give the source IP address in the respective text field.
- Click add, the respective entry will appear in the table.
- Similarly for removing an entry, select that entry from table and click remove.



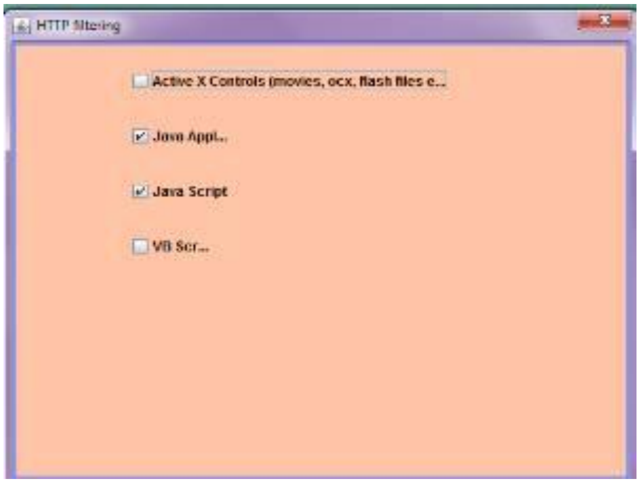
Source address: 192.168.1.0

(either IP address or Domain name)

AUTHENTICATED ADDRESSES
http://watchseries.eu

4.6. This is the **“http filtering”** dialog box

- From the Main Menu go to the proxy policies-> HTTP policies-> HTML filter, the following screen will appear.
- Check or uncheck the check boxes as per the filtering requirement.
- Click OK.



☐ Active X Controls (movies, ocx, flash files e...

☑ Java Appl...

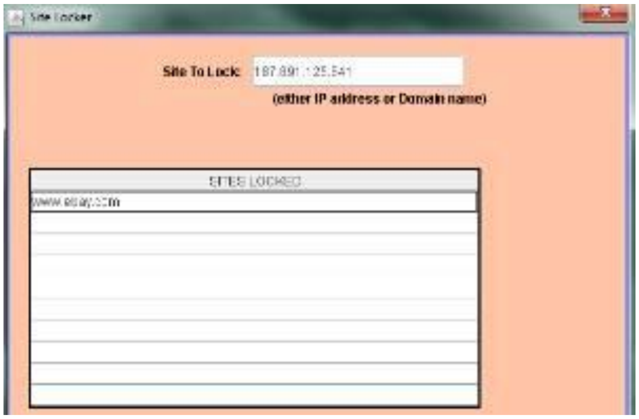
☑ Java Script

☐ VB Scr...

4.7. This is the **“site locker”** dialog box

- From the Main Menu go to the proxy policies-> HTTP policies-> HTML filter, the following screen will appear.

- Enter the site to lock.
- Click add to enter the site.
- Click remove to delete the entry.
- Click OK.



Site Locker

Site To Lock: 187.891.125.541

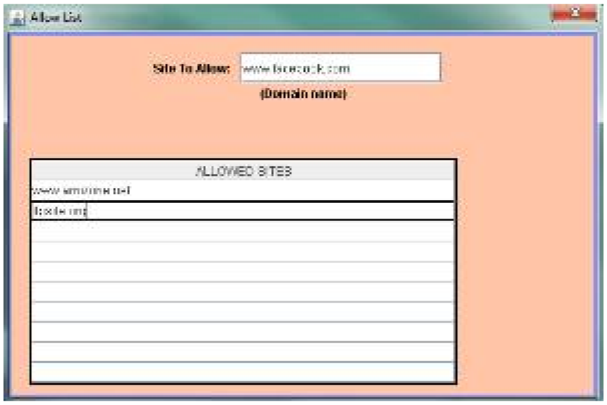
(either IP address or Domain name)

SITES LOCKED

www.ebay.com

4.8. This is the **"allow list"** dialog box.

- From the Main Menu go to the proxy policies-> HTTP policies-> site locker->Allow List, the following screen will appear.
- Enter the domain name or IP address of the site that is allowed
- Click on add, to make an entry for the site or the domain.
- Click OK.
- To remove a entry select that entry from table click Remove and then click OK



Allow List

Site To Allow: www.facebook.com

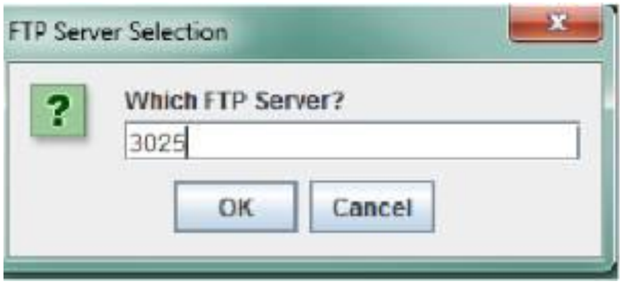
(Domain name)

ALLOWED SITES

www.amazon.net

facebook.com

4.9. This dialog box shows the **ftp server selection**. After typing the ftp server and after clicking on "OK", the ftp server starts.



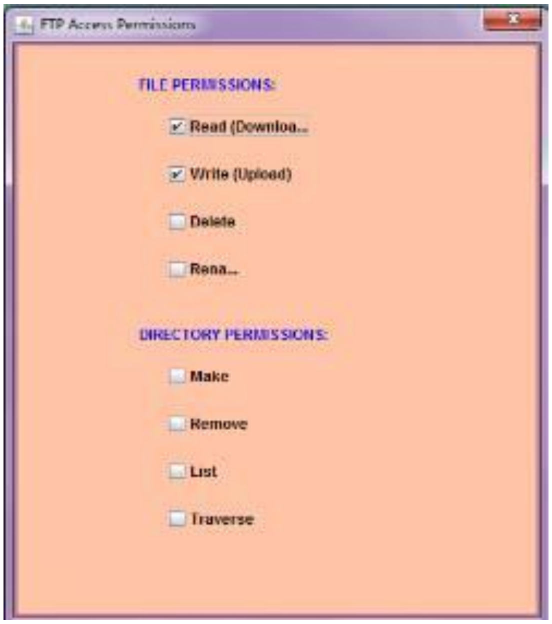
FTP Server Selection

Which FTP Server?

3025

4.10. It shows the **ftp Access permissions** options where the user can define all the accesses he wants to define for "ftp".

- From the Main Menu go to proxy policies-> FTP policies-> Allowed action settings, the following screen will appear.
- Check or Uncheck File permissions or directory permissions that are desired.
- Click OK.



FTP Access Permissions

FILE PERMISSIONS:

☑ Read (Downloa...

☑ Write (Upload)

☐ Delete

☐ Rena...

DIRECTORY PERMISSIONS:

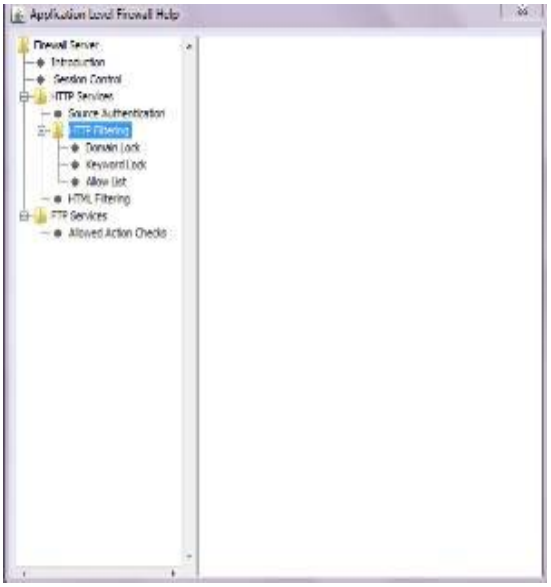
☐ Make

☐ Remove

☐ List

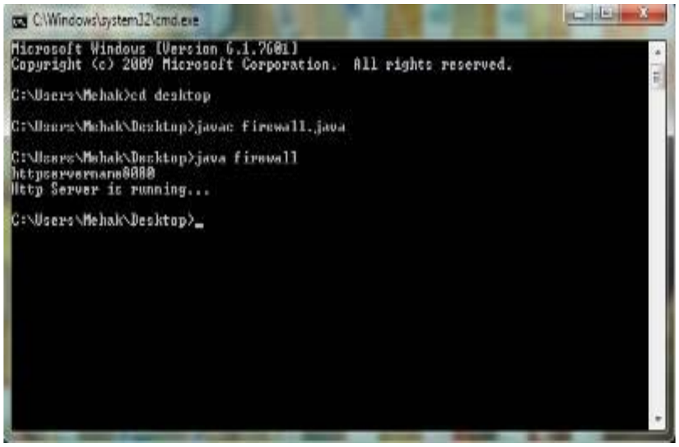
☐ Traverse

4.11. It shows the **"help"** dialog box.



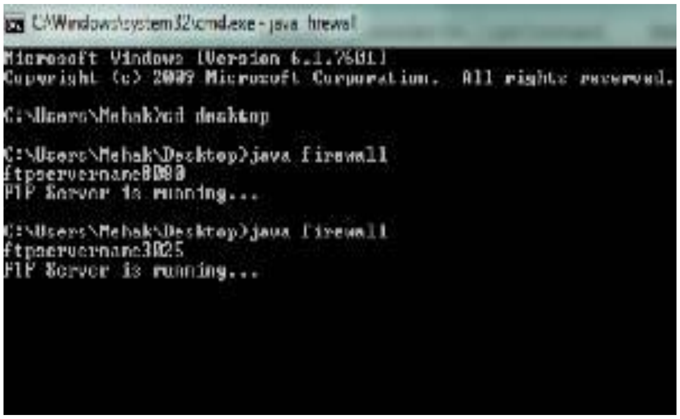
4.12. The following two outputs shows **the situation after http and ftp servers have started.**

A. WHEN HTTP SERVER IS RUNNING



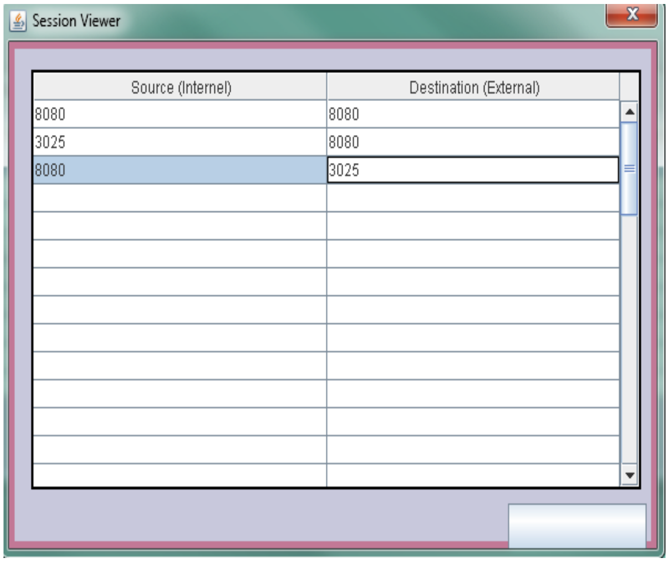
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Mehak>cd desktop

C:\Users\Mehak\Desktop>javac firewall.java

C:\Users\Mehak\Desktop>java firewall
httpservername8080
Http Server is running...

C:\Users\Mehak\Desktop>_
```

B. WHEN FTP SERVER IS RUNNING



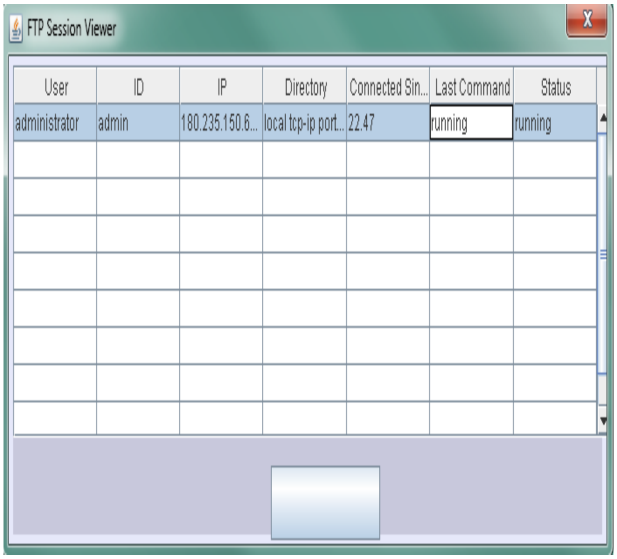
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Mehak>cd desktop

C:\Users\Mehak\Desktop>java firewall
ftpservername8080
FTP Server is running...

C:\Users\Mehak\Desktop>java firewall
ftpservername3025
FTP Server is running...
```

4.13. It shows the **http session viewer** in the firewall



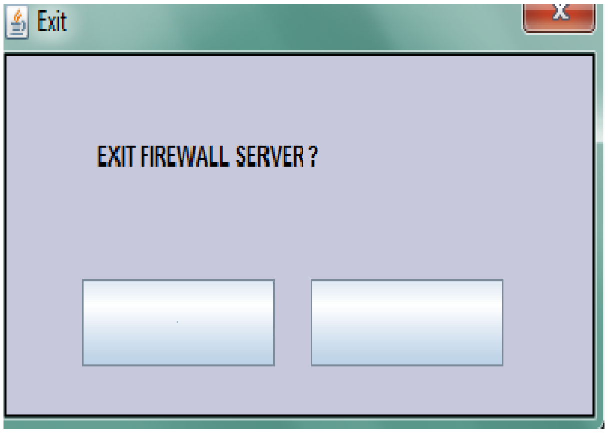
Source (Internel)	Destination (External)
8080	8080
3025	8080
8080	3025

4.15. It shows the **ftp session viewer** in firewall



User	ID	IP	Directory	Connected Sin...	Last Command	Status
administrator	admin	180.235.150.6...	local tcp-ip port...	22.47	running	running

4.16. It shows the “**close dialog box”.**



EXIT FIREWALL SERVER ?

5. CONCLUSIONS AND FUTURE IMPLICATIONS

- ❖ It can be concluded that the firewall made is sufficient enough for the following:
  - ✓ Content Filtering.
  - ✓ Blocking of client IP addresses
  - ✓
  - ✓ Blocking of web sites.
- ❖ It is recommended that the firewall can be made more effective by distributed system architecture.
- ❖ Firewall can be extended to filter images (Use of AI)
- ❖ Firewall can be extended by implementation of cryptographic protocols to make it more secure
- ❖ Firewall can be extended to work for all other ports.
- ❖ Firewall can be extended to prevent different types of denial of service attacks like “SYN” attacks, Process Table Overflow, Ping of Death.
- ❖ This proxy server can be extended as a “caching server” that will cache the pages that are frequently required by the clients in order to reduce the load on the server.

ACKNOWLEDGMENT

I would like to place on record my deep sense of gratitude to my supervisor, Er. Aniruddha Bhattacharjya, Dept. of Computer Science and Engineering, ASET, Amity University, Noida, India for his generous guidance, help and useful suggestions.

I would also acknowledge my parents for their valuable guidance and constant encouragement.

REFERENCES

[1] Herbert Schildt, ” *The Complete Reference*”, Java 2 Fifth Edition Tata McGraw Hill, New Delhi 2000.

[2] Foley and McCulley, ”*JFC Unleashed*” Techmedia.

[3] John Zukowski, “*Mastering Java 2*” BPB publications, New Delhi, 2000.

[4] D. Brent Chapman & Elizabeth D. Zwicky, “*Building Internet Firewalls*” First Edition, O’ Reily & Associates, November 1995.

AUTHOR’S BIOGRAPHY

Anukriti Raj, Student, (B-Tech 2010-2014)

Department of Computer Science & Engineering,
Amity School of Engineering & Technology, Amity
University, Noida
(U.P.) - 201303 www.amity.edu

Email id: anukritiraj.14@gmail.com

Aniruddha Bhattacharjya, Faculty Guide
Assistant Professor Grade II

E3-Block, Room No. 321,Department of Computer Science
& Engineering,
Amity School of Engineering & Technology, Amity
University, Noida
(U.P.) - 201303 www.amity.edu

Email id: abjucse@gmail.com